REMARKS/ARGUMENTS

Favorable reconsideration of this application, as presently amended and in light of the following discussion, is respectfully requested.

Claims 1, 3, 5-7, 9, 11-13, 15, 16, 18-20 and 22-26 are pending in the present application. New Claims 22-26 are added by the present amendment. Support for new Claims 22-26 can be found at least at pp. 21 and 23-26 and Figs. 9-10 of the originally filed specification. No new matter is presented.

As Applicant has not substantively amended the claims in response to any rejection of record, should a further rejection be applied in the next Action based upon newly cited prior art, Applicant submits that such an action **cannot properly be considered a Final Office Action.**

In the Office Action, Claims 1, 3, 5-7, 9, 11-13, 15, 16 and 18-20 are rejected under 35 U.S.C. § 103(a) as unpatentable over Timmer (U.S. Pub. 2002/0107895) in view of Shurts (U.S. Pat. 5,572,673).

Applicant respectfully traverses this rejection as independent Claims 1, 7, 13, 16, 19 and 20 recite novel features clearly not taught or rendered obvious by the applied references.

Independent Claim 1, for example, recites a mobile information communication device, comprising:

> ... a central control unit which ...stores metadata received through said wireless communication unit in a corresponding partition of the metadata storage unit based on matching the received metadata with a security level and/or category predetermined by the user, and *sets a higher security level for data received through a relatively secure communication path and a lower security level for other received data...*

Independent Claims 7, and 19, while directed to alternative embodiments, recite similar features. Accordingly, the remarks and arguments presented below are applicable to each of independent Claims 1, 7 and 19.

In rebutting the previously presented arguments directed to the above emphasized claimed feature, the Response to Arguments at p. 3 of the Office Action asserts that Timmer is "directed to a plurality of transmission systems used to receive data" and Shurts "teaches setting higher security levels to more sensitive data and lower security levels to less sensitive data." The Office Action then concludes that in the system of Timmer in view of Shurts "which receives and transmits data, and assigns a high security level to more sensitive data, it is only logical to assign a higher level of security to the data received in a secured communication path."

Applicant respectfully traverses this rejection, as Timmer fails to teach or suggest receiving data via both a relatively secure communication path and a communication path that is not considered as secure; and Shurts fails to teach or suggest setting security levels to data based on the path on which it was received, whatsoever. Therefore, even if combined, the references fail to teach or suggest *"set[ting] a higher security level for data received through a relatively secure communication path and a lower security level for other received data"* as recited in independent Claims 1, 7 and 19.

Timmer describes a method for creating a personalized book including content of a user's choice, such as streaming video and interactive content, in a structure designed by the user.[1] At paragraph [0019], Timmer describes that his system could be implemented in various types of networks (e.g. LAN, WAN, Internet-based, etc.).

Timmer, however, fails to teach or suggest distinguishing the type of network used to exchange data between a client and host as having different security levels, whatsoever. Moreover, Timmer clearly describes that his system is an Internet-based tool to develop an end product that "can be accessed from any location ... at any time." Thus, while Timmer does appear to disclose using a plurality of transmission systems to receive data, as asserted

---

[1] Timmer, Abstract.

in the Office Action, each of these transmission systems appear to provide an open communication path (e.g. Internet) between the client and host, and the paths are not differentiated based on security level.

Regarding <u>Shurts</u>, p. 3 of the Office Action cites col. 1, l. 1 – col. 2, l. 5 of this reference and asserts that the reference "shows an example of an object (user login account) gets configured with a clearance or sensitivity level ... [and] each data item (object) is assigned a security level to be used to enforce access control." More particularly, col. 1, l. 53 – col. 2, l. 5 of <u>Shurts</u> describes that a security policy, known as "mandatory access control" or MAC, gives "subjects" access to database objects on the basis of sensitivity labels only. A subject is an active entity, such as a user at a workstation or a command that acts on behalf of the user. An object is a passive entity that contains or receives information. Examples of objects include database tables, rows, views, and procedures. Before any object is accessed in a MAC system, the subject's sensitivity label is compared with the object's sensitivity label to determine whether the subject is allowed to access the object in the manner requested.

Thus, the cited portion of <u>Shurts</u> merely describes that a subject's sensitivity level is compared against a sensitivity level of an object being accessed in order to determine whether the subject may have a label that dominates the object. Moreover, <u>Shurts</u>, at col. 7, ll. 24-41, for example, describes that a change in the security level of an object requires an evaluation of the object by a security officer (SSO) and an initiated internal database procedure to change the status of the object. Therefore, if the system of <u>Shurts</u> were modified to assign security levels of the objects based on a path on which the object was received, it would render the system unfit for its intended purpose by taking the task of changing/assigning the security settings out of the hands of the SSO.

Therefore, <u>Shurts</u> and <u>Timmer</u>, neither alone, nor in combination, teach or suggest a mobile information communication device that includes "a central control unit which ... *sets a*

12

higher security level for data received through a relatively secure communication path and a lower security level for other received data...," as recited in amended independent Claim 1.

Accordingly, Applicant respectfully request that the rejection of Claim 1 (and the claims that depend therefrom) under 35 U.S.C. § 103 be withdrawn. For substantially similar reasons, it is also submitted that independent Claims 7 and 19 also patentably define over Timmer and Shurts.

Regarding independent Claims 13, 16 and 20, Claim 13, for example, recites an information exchange and human relation fostering support system for supporting information exchange and fostering of human relations between a plurality of users in the virtual world, comprising:

> ...at least one stationary communication device configured to acquire metadata from each mobile information communication device via a wireless transmission, *compare the acquired metadata and display the result of the comparison.*

In rejecting the above emphasized features recited in independent Claim 13, p. 5 of the Office Action asserts that the limitation of "supplies, in response to an external access request, metadata from metadata storage unit that matches a security level available to the external access request" of Claim 1 "includes matching (comparing) the metadata" as recited in Claim 13. However, this is simply not the case.

Independent Claim 1, for example, is directed to a mobile information communication device that stores metadata log information and, according to the Office Action's position, compares the security level of stored metadata with the security level of a received request. This is clearly not the same as a system including a stationary communication device that is configured to "*acquire metadata from each mobile information communication device via a wireless transmission* [and] *compare the acquired metadata* and display the result of the comparison" as recited in independent Claim 13.

The Office Action, therefore, again fails to address the above noted claim feature, and Applicant respectfully submits that Timmer and Shurts, neither alone, nor in combination, teach or suggest a stationary communication device the acquires and compared metadata, as required by independent Claims 13, 16 and 20.

Moreover, independent Claims 16 and 20 recite the additional features of:

> ... *comparing the uploaded metadata to find matching activities and interests;*
> *displaying the matching activities and interests and corresponding users discovered by the comparing;*
> *deleting the uploaded metadata from the stationary communications device.*

The Office Action also fails to address these more detailed features directed to comparing uploaded metadata, which further elaborate on the features recited in independent Claim 13. Additionally, since the outstanding Office Action has failed to address these features specifically, Applicant respectfully submits that any subsequent rejection of these features relying on rationale not articulated in the outstanding Office Action can not properly be considered a Final Office Action.

Accordingly, Applicant respectfully requests that the rejection of Claims 13, 16 and 20 (and any claims that depend therefrom) under 35 U.S.C. § 103 be withdrawn.

Further, new Claims 22-26 are added, which depend from one of independent Claims 1, 7, 13 and 19, and are allowable for at least the reasons discussed above. Furthermore, Applicant respectfully submits that dependent Claims 22-26 recite additional features clearly not taught or rendered obvious by the applied references.

Consequently, in view of the present amendment and in light of the foregoing comments, it is respectfully submitted that the invention defined by Claims 1, 3, 5-7, 9, 11-13, 15, 16, 18-20 and 22-26 is patentably distinguishing over the applied references. The present application is therefore believed to be in condition for formal allowance and an early and favorable reconsideration of the application is therefore requested.
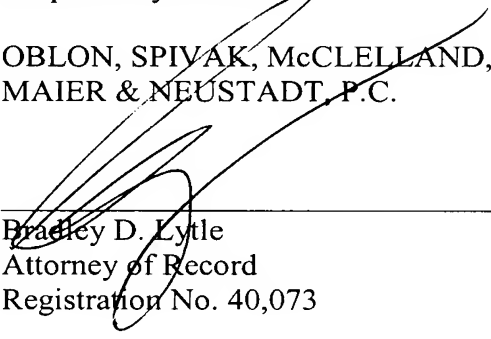
Respectfully submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.

Bradley D. Lytle
Attorney of Record
Registration No. 40,073

Customer Number

22850

Tel: (703) 413-3000
Fax: (703) 413 -2220
(OSMMN 08/07)
I:\ATTY\ATH\PROSECUTION\24S\240894US\240894US - AMD DUE 021809.DOC

Andrew T. Harry
Registration No. 56,959